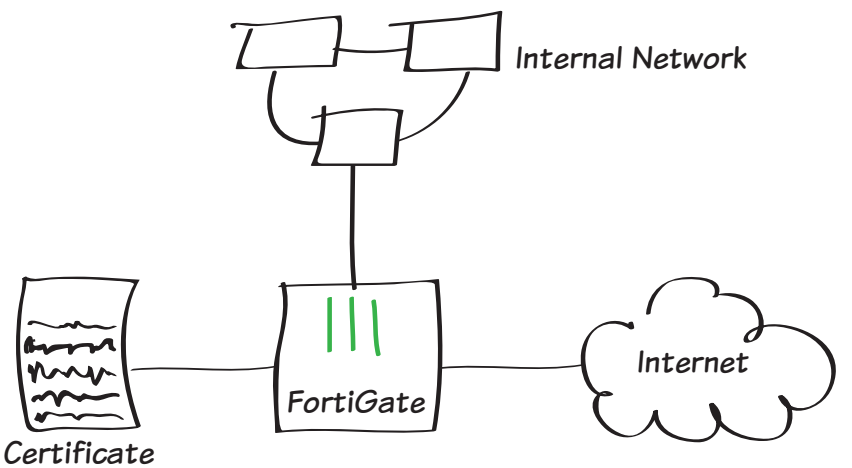
Using a custom certificate for SSL inspection

This recipe shows how use a FortiGate unit to generate a custom certificate signing request and to get this certificate signed by an enterprise root Certificate Authority (CA). This recipe also shows how to import the CA-signed certificate back into your FortiGate and how to add the certificate to an SSL inspection profile.

A certificate with *CA=TRUE* and/or *KeyUsage=CertSign* present in the metadata is necessary to perform deep inspection. By importing a custom certificate from a recognized third-party CA, you create a chain of trust that does not exist when the FortiGate's default certificate is used. This allows network users to trust the FortiGate as a CA in its own right.

1. Generating a certificate signing request (CSR)
2. Importing a signed server certificate from an enterprise root CA
3. Creating an SSL inspection profile
4. Configuring a firewall policy
5. Results



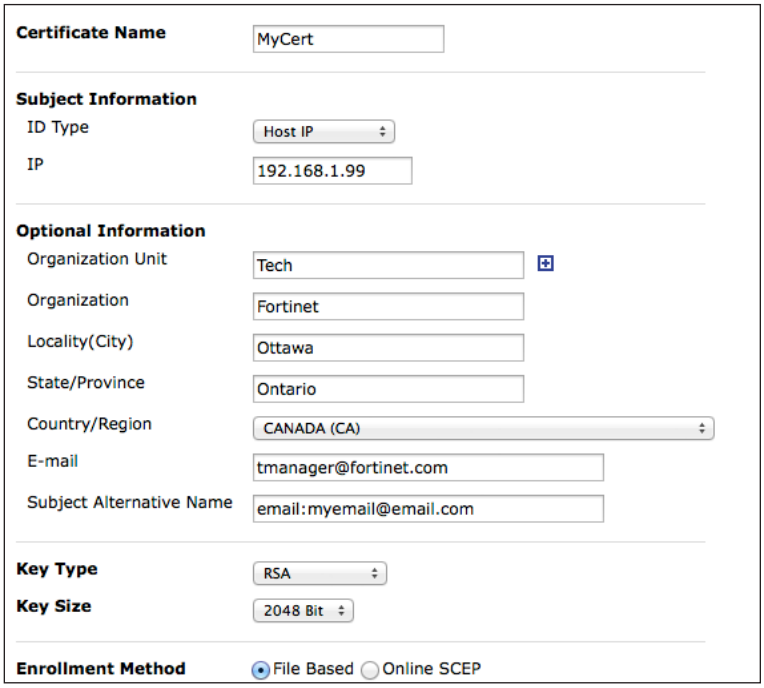
1. Generating a certificate signing request (CSR)

Go to **System > Certificates > Local Certificates** and select **Generate**.

In the **Generate Certificate Signing Request** page, fill out the required fields. You can enter a maximum of five **Organization Units**.

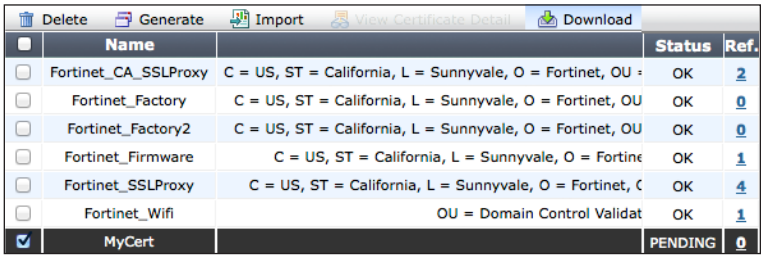
You may enter **Subject Alternative Names** for which the certificate is valid. Separate the names using commas.

To ensure PKCS12 compatibility, do not include spaces in the certificate name.



Go to **System > Certificates > Local Certificates** to view the certificate list. The status of the CSR created will be listed as **Pending.** Select the certificate and click **Download**.

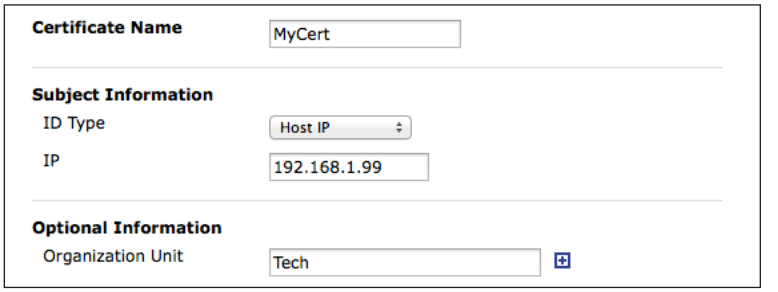
This CSR will need to be submitted and signed by an enterprise root CA before it can be used. When submitting the file, ensure that the template for a **Subordinate Certification Authority** is used.



2. Importing a signed server certificate from an enterprise root CA

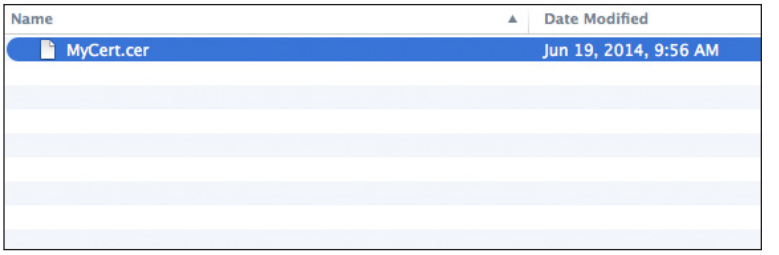
Once the CSR is signed by an enterprise root CA, you can import it into the FortiGate unit.

Go to **System > Certificates > Local Certificates** and click **Import**. From the **Type** drop down menu select **Local Certificate** and click **Choose File**.



Locate the certificate you wish to import, select it, and click **Open**.

The CA signed certificate will now appear on the **Local Certificates** list.



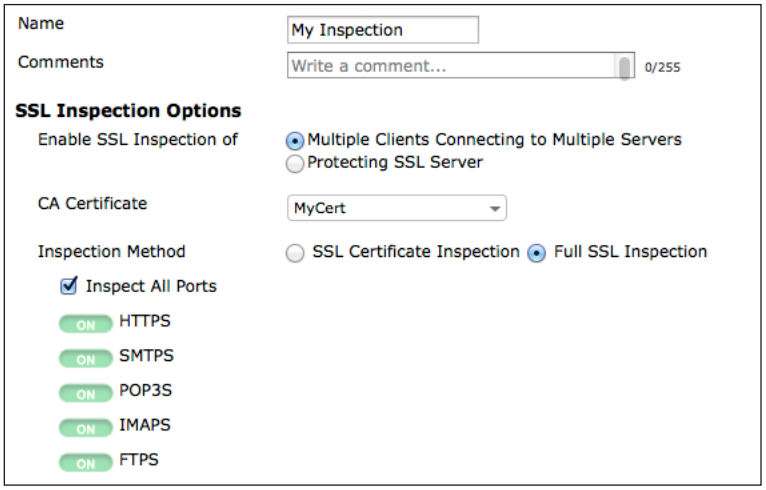
You can also use the FortiGate unit's default certificate. For information about using the default certificate, see "Preventing security certificate warnings when using SSL full inspection" on page 56.

3. Creating an SSL inspection profile

To use your certificate in an SSL inspection profile go to **Policy & Objects > Policy > SSL/SSH Inspection**.

Create a new **SSL Inspection Profile**. In the **CA Certificate** drop down menu, select the certificate you imported. Set the **Inspection Method** to **Full SSL Inspection** and **Inspect All Ports**.

You may also need to select web categories and addresses to be exempt from SSL inspection. For more information on exemptions, see “Preventing security certificate warnings when using SSL full inspection” on page 56.

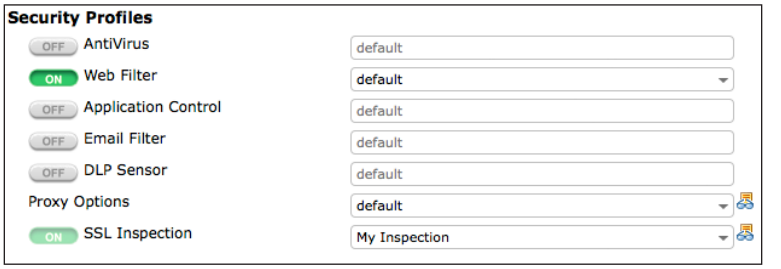


If the certificate does not appear in the list, verify that the template used to sign the certificate was for a CA and not simply for user or server identification.

4. Editing your Internet policy to use the new SSL inspection profile

Go to **Policy & Objects > Policy > IPv4** and edit the policy controlling Internet traffic.

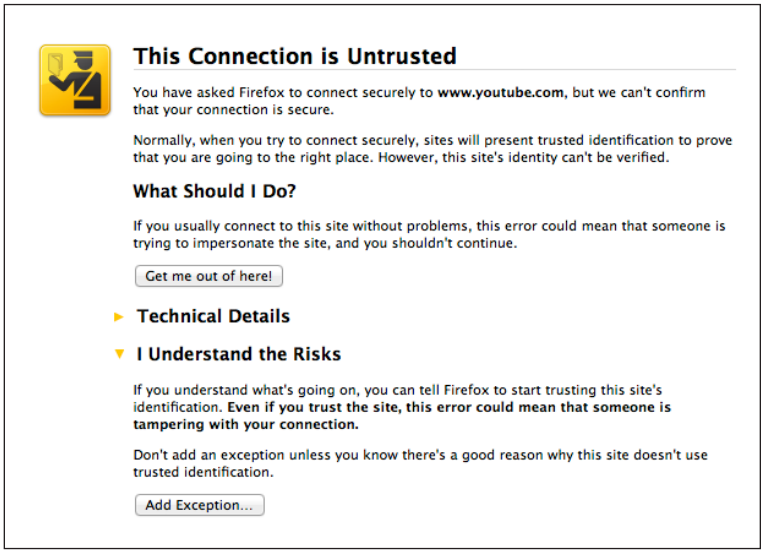
Under **Security Profiles**, ensure that **SSL Inspection** and **Web Filter** are **On**. From the **SSL Inspection** dropdown menu, select your new profile. The **Web Filter** can remain as **default**.



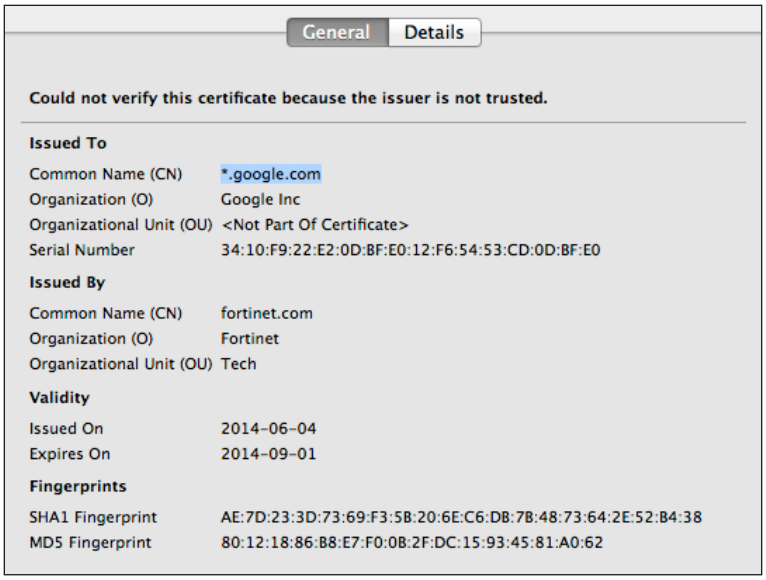
5. Results

When visiting an HTTPS website such as https://www.youtube.com/ a warning would normally appear if you are using a self-signed certificate.

If you have the correct type of certificate, signed by a recognized CA, warnings should no longer appear.



If you view the website's certificate information the **Issued By** section should contain the information of your custom certificate, indicating that the traffic is subject to deep inspection.



Network users can now manually import the certificate into their trusted root CA certificate store (IE and Chrome) and/or into their browsers (Firefox).

Alternately, if the users are members of a Windows domain, the domain administrator can use a group policy to force them to trust the self-signed certificate the FortiGate is presenting.